如何限制某一特殊用户只能执行某些操作命令

认证 会话管理 王科 2023-01-18 发表

组网及说明

通过为用户授权角色实现角色与用户的关联。将有效的用户角色成功授权给用户后，登录设备的用户才能以各角色所具有的权限来配置、管理或者监控设备。根据用户登录设备时采用的不同认证方式.。一个用户角色中可以包含多条用户角色规则，每条规则定义了是允许或禁止用户对某命令、特性、特性组、Web菜单、XML元素或者OID进行操作。

配置步骤

举例：

实现role1具有如下用户权限：

允许用户执行arp静态绑定，并可以查询此配置已生效 的权限。

```
#
role name role1
 rule 1 permit command system ; arp static *
 rule 2 permit command display current-configuration*
#
local-user h3c class manage
 password hash $h$6$hWQ/7LckAp9mFIrq$ok7ElJLku3rG9lbsqS02FtBZiZ5fCiydyerYadVZyq1WjG8c
JC0U6Xcy1z5J16mhEYVy3FmBhsTdLpImqbjlAw==
 service-type telnet
 authorization-attribute user-role role1
#
```

配置关键点

输入命令特征字符串时，需要遵循以下规则：

(1) 段（segment）的划分

¡ 若要描述多级视图下的命令，则需要使用分号（;）将命令特征字符串分成多个段，每一个段代表一个或一系列命令，后一个段中的命令是执行前一个段中命令所进入视图下的命令。一个段中可以包含多个星号（*），每个星号（*）代表了0个或多个任意字符。例如：命令特征字符串“system ; interface * ; ip * ;”代表从系统视图进入到任意接口视图后，以ip开头的所有命令。

¡ 除最后一个段外，其余段中的命令应为描述如何进入子视图的命令特征字符串。

¡ 一个段中必须至少出现一个可打印字符，不能全部为空格或Tab。

(2) 分号的使用

¡ 在输入命令特征字符串时必须指定该命令所在的视图，进入各视图的命令特征字符串由分号分隔。但是，对于能在任意视图下执行的命令（例如display命令）以及用户视图下的命令（例如dir命令），在配置包含此类命令的规则时，不需要在规则的命令匹配字符串中指定其所在的视图。

¡ 当最后一个段中的最后一个可见字符为分号时，表示所指的命令范围不再扩展，否则将向子视图中的命令扩展。例如：命令特征字符串“system ; radius scheme * ;”代表系统视图下以radius scheme开头的所有命令；命令特征字符串“system ; radius scheme * ”代表系统视图下以radius scheme开头的所有命令，以及进入子视图（RADIUS方案视图）下的所有命令。

(3) 星号的使用

¡ 当星号（*）出现在一个段的首部时，其后面不能再出现其它可打印字符，且该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“system ; *”就代表了系统视图下的所有命令，以及所有子视图下的命令。

¡ 当星号（*）出现在一个段的中间时，该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“debugging * event”就代表了用户视图下所有模块的事件调试信息开关命令。